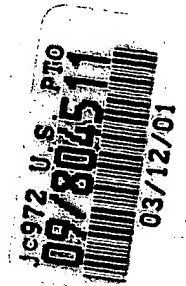


501PD364US00

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出 願 年 月 日  
Date of Application:

2000年 8月25日

願 番 号  
Application Number:

特願2000-260864

願 人  
Applicant(s):

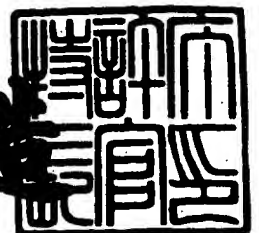
ソニー株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2000年12月22日

特許庁長官  
Commissioner,  
Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 0000608605

【提出日】 平成12年 8月25日

【あて先】 特許庁長官殿

【国際特許分類】 H04K 1/00

【発明者】

    【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
内

    【氏名】 市村 元

【特許出願人】

    【識別番号】 000002185

    【氏名又は名称】 ソニー株式会社

    【代表者】 出井 伸之

【代理人】

    【識別番号】 100086841

    【弁理士】

    【氏名又は名称】 脇 篤夫

【代理人】

    【識別番号】 100114122

    【弁理士】

    【氏名又は名称】 鈴木 伸夫

【手数料の表示】

    【予納台帳番号】 014650

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

    【包括委任状番号】 9710074

【包括委任状番号】 0007553

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ送出装置、データ復号装置、データ送出方法、データ復号方法、伝送システム

【特許請求の範囲】

【請求項 1】 一連の連続したデータ列のプログラムを暗号化して送出するデータ送出装置において、

ランダムノイズを発生するランダムノイズ発生手段と、

上記ランダムノイズ発生手段で発生したランダムノイズを上記プログラムの前後に付加する付加手段と、

上記付加手段にてランダムノイズが付加されたプログラムに対して暗号化処理を行う暗号化手段と、

上記暗号化手段により暗号化されたランダムノイズが付加されたプログラムを送出する送出手段と、

を備えたことを特徴とするデータ送出装置。

【請求項 2】 上記送出手段は、有線又は無線で接続された他の機器に対して上記プログラムを送出することを特徴とする請求項 1 に記載のデータ送出装置。

【請求項 3】 上記送出手段は、上記プログラムを記録媒体に記録するデータとして送出することを特徴とする請求項 1 に記載のデータ送出装置。

【請求項 4】 上記付加手段で付加するランダムノイズのデータ長は可変長とされていることを特徴とする請求項 1 に記載のデータ送出装置。

【請求項 5】 一連の連続したデータ列の前後にランダムノイズが付加され、暗号化が施されたプログラムを入力して復号するデータ復号装置において、

送出されてきたプログラムを入力する入力手段と、

上記入力手段により入力されたプログラムに対して暗号化を解読する復号処理を行う復号手段と、

上記復号手段で復号されたプログラムの前後に付加されているランダムノイズを除去する除去手段と、

を備えたことを特徴とするデータ復号装置。

【請求項 6】 上記入力手段は、有線又は無線で接続された他の機器から送出されてきたプログラムを入力することを特徴とする請求項 5 に記載のデータ復号装置。

【請求項 7】 上記入力手段は、記録媒体から読み出されて送出されてきたプログラムを入力することを特徴とする請求項 5 に記載のデータ復号装置。

【請求項 8】 一連の連続したデータ列のプログラムの前後にランダムノイズを付加し、

ランダムノイズが付加されたプログラムに対して暗号化処理を行ない、

暗号化されたランダムノイズが付加されたプログラムを送出することを特徴とするデータ送出方法。

【請求項 9】 プログラムの前後に付加するランダムノイズのデータ長は可変長とされていることを特徴とする請求項 8 に記載のデータ送出方法。

【請求項 10】 一連の連続したデータ列の前後にランダムノイズが付加され、暗号化が施されたプログラムを入力し、

入力されたプログラムに対して暗号化を解読する復号処理を行ない、

復号されたプログラムの前後に付加されているランダムノイズを除去することを特徴とするデータ復号方法。

【請求項 11】 一連の連続したデータ列のプログラムを暗号化して送出するデータ送出装置と、送出されてきたプログラムを復号する復号装置から成る伝送システムにおいて、

上記データ送出装置は、

ランダムノイズを発生するランダムノイズ発生手段と、

上記ランダムノイズ発生手段で発生したランダムノイズを上記プログラムの前後に付加する付加手段と、

上記付加手段にてランダムノイズが付加されたプログラムに対して暗号化処理を行う暗号化手段と、

上記暗号化手段により暗号化されたランダムノイズが付加されたプログラムを送出する送出手段と、

を備え、

上記データ復号装置は、  
送出されてきたプログラムを入力する入力手段と、  
上記入力手段により入力されたプログラムに対して暗号化を解読する復号処理を行う復号手段と、  
上記復号手段で復号されたプログラムの前後に付加されているランダムノイズを除去する除去手段と、  
を備えたことを特徴とする伝送システム。

【請求項 1 2】 上記付加手段で付加するランダムノイズのデータ長は可変長とされていることを特徴とする請求項 1 1 に記載の伝送システム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は暗号化されたプログラムデータの伝送を行う伝送システム、及びパケットデータの伝送にかかるデータ送出装置、データ復号装置、データ送出方法、データ復号方法に関するものである。

【0 0 0 2】

【従来の技術】

例えば著作権保護が必要なデータ、秘密性の高いデータ、プライバシーにかかる私的データなど、外部に漏洩することが好ましくないデータの伝送に際しては、暗号化処理が行われることが多い。例えば音楽データ、映像データなど、一連の連続したデータ列としてのプログラムの伝送に際しては、著作権保護の必要性などから暗号化が行われて伝送されることが行われている。なお、本明細書でいう「プログラム」とは、一連のデータ列としてデータ群のことであり、例えば一般に 1 つの楽曲のデータに相当する「トラック」とも呼ばれるものを含む広義のものである。

【0 0 0 3】

図 1 1 に或る送信装置 1 0 1 から受信装置 1 0 2 に対してプログラムデータを暗号化して伝送するモデルを示す。

いま、伝送しようとするデータ D T が送信装置 1 0 1 に入力されたとすると、

送信装置 1 0 1 は、まず暗号化部 1 1 1 で暗号化処理を施し、暗号化されたデータ D T s を生成する。

そしてそのデータ D T s は送信部 1 1 2 から送信出力される。

送信出力されたデータ D T s は例えば I E E E 1 3 9 4 バスなどの伝送路 1 0 3 により、受信装置 1 0 2 に送られることになる。

受信装置 1 0 2 では、伝送路 1 0 3 から送信されてきたデータ D T s を受信部 1 2 1 で受信し、復号部 1 2 2 で暗号解読処理を行うことで、元のデータ D T を得ることができる。

#### 【 0 0 0 4 】

##### 【発明が解決しようとする課題】

このように伝送路 1 0 3 においては暗号化されたデータ D T s が送信されることで、仮に伝送路 1 0 3 においてデータ D T s が取り出されたとしても、データ D T の内容は秘密性が保たれるものとなる。

しかしながら、例えば著作権保護を目的として音楽データ等を図 1 1 のようなシステムで伝送する場合、暗号を解読され、結果として違法なコピーが行われるおそれがある。

#### 【 0 0 0 5 】

例えば伝送しようとするプログラムとしてのデータ D T が P C M オーディオデータであったとする。

P C M オーディオデータの場合、無音部分では、データストリーム上でゼロデータが並んでいるものとなっている。又は例えば  $\Delta \Sigma$  変調された 1 ビットオーディオデータの場合、無音部分は「9 6 h」 (= 1 0 0 1 0 1 1 0) などの固定パターンとなっている。

音楽トラックとしてのプログラムデータを考えると、そのプログラムの先頭部分と終端部分は、多くの場合、無音となっている。つまり、例えば 2 つの曲（プログラム）が、音楽としてメドレー形式でつながっている場合などを除いては、曲の頭（曲が開始される直前）と終わり（曲が終了した直後）はデータとしては無音部分が存在していることが殆どである。

## 【0006】

ここで、図11に破線で示すように、何らかの手段で伝送路103から暗号化されたデータDTsが取り出されたとする。

通常は、データDTsを解析しても、元のデータDT自体がわからないため、暗号の解読は困難である。

ところが、データDTsにおいて、プログラムデータDTのうちで曲の先頭部分又は終端部分、即ち無音部分に相当する部分を抽出されると、元のデータがゼロデータ等の固定パターンであること、つまり元のデータの内容が明白となっている場合が多いことから、比較的容易に暗号が解読され、データDTの内容や暗号化アルゴリズムが知られてしまう危険性がある。

もちろん暗号化アルゴリズムが解読されれば、悪意のユーザーによればその後データDTの違法な取り込みが容易に可能となってしまう。つまり著作権侵害となるような行為を実行可能としてしまう。

## 【0007】

従って、音楽データ等の著作権保護が必要なデータについて、機器間の伝送、記録媒体への記録のための伝送、或いは公衆回線等を用いた音楽配信システムにおける伝送などの広範囲の分野で、上記の危険性が内包されており、このため違法な暗号解読を防止できるような技術が求められている。

## 【0008】

## 【課題を解決するための手段】

本発明はこのような状況に鑑みて、伝送されるデータについて、容易に暗号解読ができないようにする技術を提供するものである。

## 【0009】

このため本発明では、一連の連続したデータ列のプログラムを暗号化して送出するデータ送出装置において、ランダムノイズを発生するランダムノイズ発生手段と、上記ランダムノイズ発生手段で発生したランダムノイズを上記プログラムの前後に付加する付加手段と、上記付加手段にてランダムノイズが付加されたプログラムに対して暗号化処理を行う暗号化手段と、上記暗号化手段により暗号化されたランダムノイズが付加されたプログラムを送出する送出手段とを備えるよ



うにする。

また、上記付加手段で付加するランダムノイズのデータ長は可変長とされているようにする。

#### 【0010】

また本発明は、一連の連続したデータ列の前後にランダムノイズが付加され、暗号化が施されたプログラムを入力して復号するデータ復号装置において、送出されてきたプログラムを入力する入力手段と、上記入力手段により入力されたプログラムに対して暗号化を解読する復号処理を行う復号手段と、上記復号手段で復号されたプログラムの前後に付加されているランダムノイズを除去する除去手段とを備える。

#### 【0011】

また、本発明の伝送システムは、上記構成のデータ送出装置と上記構成のデータ復号装置により構成されるものとする。

そしてデータ送出装置とデータ復号装置は、それぞれ異なる機器間における送信装置、受信装置としたり、記録媒体に記録を行う記録装置における記録データの送出装置、記録媒体からデータの再生を行う再生装置における再生データの復号装置などとして実現されるようにする。

#### 【0012】

本発明のデータ伝送方法は、一連の連続したデータ列のプログラムの前後にランダムノイズを付加し、ランダムノイズが付加されたプログラムに対して暗号化処理を行ない、暗号化されたランダムノイズが付加されたプログラムを送出する。

ここで、プログラムの前後に付加するランダムノイズのデータ長は可変長とする。

本発明のデータ復号方法は、一連の連続したデータ列の前後にランダムノイズが付加され、暗号化が施されたプログラムを入力し、入力されたプログラムに対して暗号化を解読する復号処理を行ない、復号されたプログラムの前後に付加されているランダムノイズを除去する。

## 【0013】

即ち本発明では、暗号化を行う前にプログラム（曲データ等）の前後にランダムノイズを付加する。これによって、例えば元のデータにおいて曲の前後に無音部分が存在しても、ランダムノイズが付加されることで曲の先頭及び終端が無音データとはならない状態とされた上で暗号化されることとなるため、暗号化されたプログラムの先頭部分又は終端部分が抽出されて解析されても、暗号アルゴリズムの解読は非常に困難なものとなる。また付加するランダムノイズのデータ長は可変長とすることで無音データ部分が位置的に不明確になり、暗号解読防止効果を高めることができる。

## 【0014】

## 【発明の実施の形態】

以下、本発明の実施の形態を次の順に説明する。

1. 送信装置及び受信装置に本発明を採用する例
2. IEEE 1394 の伝送フォーマット
3. IEEE 1394 でのデータ伝送の場合のランダムノイズ付加例
4. 記録装置及び再生装置に本発明を採用する例

## 【0015】

1. 送信装置及び受信装置に本発明を採用する例

本発明のデータ送出装置（データ送出方法）、データ復号装置（データ復号方法）を、送信装置、受信装置に採用する実施の形態を説明する。

図1は、或る2つの機器が例えばIEEE 1394バスによる伝送路3により接続されている場合に、送信装置1を有する機器から受信装置2を有する機器にプログラムデータDTを伝送するモデルにおいて本発明の実施の形態を示したものである。

詳しくは後述するが、データDTは、例えば1ビットデジタルオーディオデー

タを、所定の伝送プロトコルに合致するフォーマットに基づいてパケット化（ブロック化）したものであるとする。

#### 【 0 0 1 6 】

1ビットデジタルオーディオデータとは、通常のCD（Compact Disc）におけるオーディオデータよりも高品位なデータとして開発されたものであり、サンプリング周波数を例えばCD方式における44.1KHzの16倍という非常に高いサンプリング周波数である2.842MHzとして $\Delta\Sigma$ 変調された1ビットデータのことであり、周波数帯域はDC成分～100KHzの広範囲とされ、ダイナミックレンジはオーディオ帯域全体で120（dB）を実現できるデータ形式である。

なお、本例ではこのような1ビットデジタルオーディオデータをパケット化して伝送する場合を例に挙げるが、もちろん伝送されるデータ自体の形式、種別はどのようなものでもよい。

#### 【 0 0 1 7 】

図示するように送信装置1は、ランダムノイズ付加部11、暗号化部12、送信部13、ランダムノイズ発生部14が設けられる。

ランダムノイズ発生部14は例えば乱数発生回路によりランダムノイズ（乱数データ）を発生させ、ランダムノイズ付加部11に供給する。

ランダムノイズ付加部11は、送信しようとするデータDTに対して、プログラム（楽曲等）の先頭部分及び終端部分に、上記ランダムノイズ発生部14で発生されたランダムノイズを付加する動作を行う。

暗号化部12は、ランダムノイズ付加部11の出力に対して所定の暗号アルゴリズムでの暗号化処理を施す。

送信部13は暗号化部12の出力をIEEE1394バスによる伝送路3に送出する動作を行う。

#### 【 0 0 1 8 】

受信装置2は、受信部21、復号部22、ランダムノイズ除去部23を備える。

受信部21は、伝送路3から供給されるデータを受信して取り込む動作を行う。

。復号部 2 2 は、上記暗号化部 1 2 での暗号化アルゴリズムに対応して暗号解読処理を行う部位である。

ランダムノイズ除去部 2 3 は、上記ランダムノイズ付加部 1 1 で付加されたランダムノイズ部分を除去する部位である。

#### 【 0 0 1 9 】

このような送信装置 1、受信装置 2 においてデータ D T の伝送は次のように行われる。図 2 を参照しながら説明する。

図 2 ( a ) はプログラム（トラック）として 1 曲が構成されている楽曲データを示している。これがデータ D T として伝送しようとするオーディオデータソースである。そして音楽データの場合、トラックデータの先頭部分と終端部分は図 2 ( b ) のように無音となっている場合が多い。

#### 【 0 0 2 0 】

例えば楽曲等のプログラムデータとして、図 2 ( a ) ( b ) に示すデータ D T が送信装置 1 に入力されたとすると、送信装置 1 は、まずランダムノイズ付加部 1 1 で、データ D T におけるプログラムの先頭及び終端に相当する部分に、任意のデータ長としてのランダムノイズを挿入する。例えば図 2 ( c ) のように、トラックの先頭部分に時間長 T a d 1 のデータサイズのランダムノイズを付加し、またトラックの終端部分に時間長 T a d 2 のデータサイズのランダムノイズを付加する。具体例は後述するが、例えばランダムノイズが充填されたブロックをパケットデータに付加する。

なお、時間長 T a d 1、T a d 2、即ち付加するランダムノイズのデータ長は、一定としてもよいが、可変長、即ち付加処理を行うたびに毎回ランダムな長さとしたり、送信装置 1 としての機器毎に任意に設定する長さとしてもよい。付加するランダムノイズのデータ長のランダム性が高いほど、実際の無音データ部分がより不明確となるため、不正な暗号解読をより困難にできる。

#### 【 0 0 2 1 】

ランダムノイズ付加部 1 1 でランダムノイズが付加されたデータ D T a d は、続いて暗号化部 1 2 に供給され、暗号化処理が施される。即ち図 2 ( d ) のよう

に、ランダムノイズ部分、無音を含めた音楽データ部分が、それぞれ暗号化された状態となる。

暗号化されたデータ D T s は、送信部 1 3 に供給され、送信部 1 3 から伝送路 3 に対して送出されることになる。

#### 【 0 0 2 2 】

このように送信されたデータ D T s を受信する受信装置 2 では、まず伝送路 3 から供給されてきたデータ D T s を受信部 2 1 で受信し、復号部 2 2 に供給する。復号部ではデータ D T s に対する暗号解読処理を行うことで、暗号化前のデータ、即ち図 2 ( c ) のようにランダムノイズが付加されている状態のデータ D T a d が出力される。

このデータ D T a d はランダムノイズ除去部 2 3 に供給され、ランダムノイズ部分が除去されることで、当初の送信データ、即ち図 2 ( b ) のようなデータ D T が得られることとなる。

#### 【 0 0 2 3 】

ここで図 1 に破線で示すように、何らかの手段で伝送路 3 から暗号化されたデータ D T s が取り出された場合を考える。

上述したようにデータ D T s において元の内容が明白な無音部分が抽出されると暗号化アルゴリズムが解読されるおそれがある。そして無音部分としては通常、トラックの先頭部分及び終端部分である。従って、データ D T s においてトラックの先頭部分又は終端部分に相当する部分が不正な暗号解読に用いられると、暗号解読に有利となってしまう。

#### 【 0 0 2 4 】

しかしながら本例の場合、データ D T s は、トラックの先頭及び終端にランダムノイズが付加された上で暗号化されたものである。つまりトラックの先頭及び終端はゼロデータ等の固定パターンが連続する部分ではないものとされた状態で暗号化されている。従ってデータ D T s においてトラックの先頭又は終端に相当する部分が抽出されたとしても、元のデータはランダムノイズであることから、元のデータは予測できず、暗号解読は困難となる。

特にデータ D T s の解析処理において、データ D T s 上では暗号化アルゴリズム

ムによるデータ要素とランダムノイズによるデータ要素を区別することはできず、暗号化アルゴリズムを解析することはほぼ不可能である。

さらに、付加するランダムノイズのデータ長が可変長であることで、不正な解読を行おうとする者が、実際のゼロデータもしくは固定パターンが連続する部分を予測することは著しく困難となり、この点で暗号解読に対する安全性を高めることができる。

#### 【0025】

以上のことから、本例によれば伝送路3で伝送されるデータについて暗号解読は非常に困難なものとなり、従って、著作権保護を要するデータの伝送などに非常に好適なものとなる。

また送信装置1側では従前の構成にランダムノイズ付加部11及びランダムノイズ発生部14を設けるだけでよく、受信装置2側では、ランダムノイズ除去部23を設けて、暗号化を解読したうえでランダムノイズが挿入されたデータ部分を除去するのみでデータを復号できる。従って送信装置1、受信装置2としての構成がさほど複雑化することもなく、各種の機器への導入は容易なものとなる。

#### 【0026】

## 2. IEEE1394の伝送フォーマット

ここでIEEE1394による伝送フォーマットについて説明する。

IEEE1394方式でのデータ伝送では、例えば図3(a)に示すように、所定の通信サイクル(例えば $125\mu\text{sec}$ )毎に時分割多重によって行われる。そして、この信号の伝送は、サイクルマスタと呼ばれる機器(IEEE1394バス上の任意の1台の機器)が通信サイクルの開始時であることを示すサイクルスタートパケットCSPをバス上へ送出することにより開始される。なお、サイクルマスタは、バスを構成するケーブルに各機器を接続したとき等に、IEEE1394で規定する手順により自動的に決定される。

## 【 0 0 2 7 】

1 通信サイクル中における通信の形態は、ビデオデータやオーディオデータなどのリアルタイム性を必要とするデータを伝送するアイソクロナス伝送 ( I s o ) と、制御コマンドや補助的なデータなどを確実に伝送するアシンクロナス伝送 ( A s y ) の 2 種類の伝送が行われる。

各通信サイクル中では、アイソクロナス伝送用のアイソクロナスパケット I s o が、アシンクロナス伝送用のアシンクロナスパケット A s y より先に伝送される。

アイソクロナスパケット I s o の通信が終了した後、次のサイクルスタートパケット C S P までの期間が、アシンクロナスパケット A s y の伝送に使用される。従って、アシンクロナスパケット A s y が伝送できる期間は、そのときのアイソクロナスパケット I s o の伝送チャンネル数により変化する。また、アイソクロナスパケット I s o は、1 通信サイクル毎に予約した帯域 ( チャンネル数 ) が確保される伝送方式であるが、受信側からの確認は行わない。

アシンクロナスパケット A s y で伝送する場合には、受信側からアクノリッジメント ( A c k ) のデータを返送させて、伝送状態を確認しながら確実に伝送させる。

## 【 0 0 2 8 】

図 3 ( b ) に、C I P ( Common Isochronous Packet ) の構造を示す。つまり、図 3 ( a ) に示したアイソクロナスパケット I s o のデータ構造である。

例えば、上述した 1 ビットデジタルオーディオデータは、 I E E E 1 3 9 4 通信においては、アイソクロナス通信によりデータの送受信が行われる。つまり、リアルタイム性が維持されるだけのデータ量をこのアイソクロナスパケットに格納して、1 アイソクロナスサイクル毎に順次送信するものである。

## 【 0 0 2 9 】

アイソクロナスパケットは、図 3 ( b ) のように、1 3 9 4 パケットヘッダ、ヘッダ C R C 、 C I P ヘッダ、データ部、データ C R C から成る。

この C I P 構造として、例えば 2 チャンネルの 1 ビットデジタルオーディオデータの伝送に用いる場合における具体例を図 4 に示している。

## 【0030】

図4では、横方向に32ビット（4バイト）を示しているが、その1行分のデータ、つまり32ビットが1カドレット（quadlet）と呼ばれる。

CIPの先頭32ビット（1カドレット）は、1394パケットヘッダとされている。

1394パケットヘッダにおいては、16ビットのデータレングス（data\_Leng t h）、2ビットのタグ（t a g）、6ビットのチャンネル（c h a n n e l）、4ビットのタイムコード（t c o d e）、4ビットのシンク（s y）が配される。

そして、1394パケットヘッダに続く1カドレットの領域はヘッダCRCが格納される。

## 【0031】

ヘッダCRCに続く2カドレットの領域がCIPヘッダとなる。

CIPヘッダの上位カドレットの先頭2バイトには、それぞれ‘0’ ‘0’が格納され、続く6ビットの領域はSID（送信ノード番号）を示す。SIDに続く8ビットの領域はDBS（データブロックサイズ）であり、データブロックのサイズ（パケット化の単位データ量）が示される。続いては、FN（2ビット）、QPC（3ビット）の領域が設定されており、FNにはパケット化する際に分割した数が示され、QPCには分割するために追加したカドレット数が示される。

SP（1ビット）にはソースパケットのヘッダのフラグが示され、DBCにはパケットの欠落を検出するカウンタの値が格納される。

なお、図中「r s v」はリザーブ、つまり未定義の領域を示している。

## 【0032】

CIPヘッダの下位カドレットの先頭2バイトにはそれぞれ‘1’ ‘0’が格納される。そして、これに続いてFMT（6ビット）、FDF（8ビット）、SYT（16ビット）の領域が設けられる。

FMTには信号フォーマット（伝送フォーマット）が示され、ここに示される値によって、当該CIPに格納されるデータ種類（データフォーマット）が識別



可能となる。具体的には、MPEGストリームデータ、Audioストリームデータ、デジタルビデオカメラ（DV）ストリームデータ等の識別が可能になる。

FDFは、フォーマット依存フィールドであり、上記FMTにより分類されたデータフォーマットについて更に細分化した分類を示す領域とされる。オーディオに関するデータであれば、例えばリニアオーディオデータであるのか、MIDIデータであるのかといった識別が可能になる。

例えば1ビットデジタルオーディオデータであれば、先ずFMTによりAudioストリームデータの範疇にあるデータであることが示され、FDFに規定に従った特定の値が格納されることで、そのAudioストリームデータは1ビットデジタルオーディオデータであることが示される。

SYTは、フレーム同期用のタイムスタンプが示される。

#### 【0033】

このようなCIPヘッダに続けては、FMT、FDFによって示されるデータが、データ部としてのn個のデータブロック（ブロック#0～#n）のシーケンスによって格納される。FMT、FDFにより1ビットデジタルオーディオデータであることが示される場合には、このデータブロックとしての領域に1ビットデジタルオーディオデータが格納される。

そして、データブロックに続いて最後にデータCRCが配置される。

#### 【0034】

この図4では、データ部に2チャンネルの1ビットデジタルオーディオデータが配されている例を示している。これは、IEEE1394バスによるデータ伝送について適用できるAM824と呼ばれる伝送プロトコルに基づいた例であり、その場合において1ビットデジタルオーディオデータとして2チャンネルのオーディオデータを伝送する場合のパケット構造例である。

#### 【0035】

上述のように32ビット（4バイト）を1カドレット（Quadlet）と呼ぶとすると、2チャンネルデータの場合、4カドレット（q1～q4）で1つのブロックが形成され、このブロックが連続するものとなる。

## 【0036】

各カドレットにおける先頭のバイト（バイト0）は、ラベルとされている。ラベルとは、そのカドレットに配されるデータの識別情報となる。

ラベルとしての値及び意味を図5に示す。

図示するようにラベル値に対して各種の意味が定義されており、例えばラベル値40h～4Fhは、DVD（Digital Versatile Disc）システムで採用されているマルチビットリニアオーディオデータに対応するものとされる。なお、「h」を付した数値は16進表記のものである。

またラベル値50h～57hは、1ビットデジタルオーディオデータに対応する値、ラベル値58h～5Fhは、エンコードされた1ビットデジタルオーディオデータに対応する値、ラベル値80h～83hはMIDIデータに対応する値とされる。

さらにC0h～EFhはアンシラリデータ（Ancillary Data；補助データ）を意味するなど、ラベル値は識別情報として機能するために各種定義されている。

## 【0037】

各ラベル値についての詳細な定義の説明は本発明と直接関係がないため説明を省略するが、図4に示した値についてのみ述べると次のようになる。

## 【0038】

図4においてブロック#0の第1カドレットq1をみると、ラベル値は「D1h」とされている。従って第1カドレットq1はアンシラリデータが記述されるものと提示されていることになり、さらにこの場合バイト1はサブラベルとされて「00h」とされている。

このときバイト2、バイト3が実際の補助データ内容となるが、ここではバリディティフラグ（Validity Flag）V、コピーコントロール情報（Track Attribute）、チャンネル数（Ch Bit Num）、スピーカ配置情報（Loudspeaker Config）が記述される。

## 【0039】

第2カドレットq2ではラベル値は「50h」とされる。ラベル値50h～57hは、1ビットデジタルオーディオデータに対応する値であるが、「50h」

は、マルチチャンネルのデータを配したブロックの最初のデータであることを示す。

また第3カドレット q 3 ではラベル値は「5 1 h」とされる。「5 1 h」は、マルチチャンネルのデータを配したブロックの2番目以降のデータであることを示す。

従って、第2、第3カドレット (q 2、q 3) では、チャンネル1、チャンネル2の2チャンネルの1ビットデジタルオーディオデータが配されていることが示されるものとなる。各チャンネルのデータはバイト1～バイト3の3バイトで記述される。

#### 【0 0 4 0】

第4カドレット q 4 では、ラベル値は「C F h」とされている。これはアンシラリデータの範疇であるが、「C F h」は特に無効データ (NO DATA) を示す値として定義されている。またバイト1はサブラベルとして無効データの内容を示す値とされており、この例では「C F h」とされている。

そしてこのときバイト2、バイト3が無効データにより充填される。

#### 【0 0 4 1】

ブロック#1の第1カドレット q 1 では、ラベル値は「D 1 h」とされている。従って第1カドレット q 1 はアンシラリデータが記述されるものと提示されていることになり、さらにこの場合バイト1はサブラベルとされて「0 1 h」とされている。

このときはバイト2、バイト3の補助データ内容は、サブリメンタリデータとされる。

第2～第4カドレットはブロック#0と同様である。

#### 【0 0 4 2】

このように各ブロックが構成されて、アイソクロナスパケット I s o におけるデータ部が形成される。

#### 【0 0 4 3】

### 3. IEEE 1394でのデータ伝送の場合のランダムノイズ付加例

以上のようなIEEE 1394による伝送フォーマットを用いて、図1で説明したようにデータを伝送する場合の具体例を以下、説明していく。即ちIEEE 1394の伝送路3でオーディオパケットデータを伝送する場合のランダムノイズ付加方式の例である。

#### 【0044】

上記図4で示したデータ部を構成するブロック#0、#1・・・に配されるオーディオデータは、元々の1ビットデジタルオーディオデータとしてのプログラムから見ると図6に示す関係となる。

図6(a)は1つの楽曲としてのデータ群となるトラック(プログラム)をトラック#Nとして示しているが、このトラック#Nは図6(b)のように複数のフレームから構成される。

公知のように1つのフレームは75Hz周期、即ち13.3msec分のオーディオデータに相当する単位である。

そして図6(c)のように1フレームは1568ブロック(ブロック#0～#1567)で構成される。

#### 【0045】

図7は送信しようとするデータDTとしてのデータパケット構造例を示している。これは、IEEE 1394バスによるデータ伝送について適用できるAM824の伝送プロトコルに基づき、1ビットデジタルオーディオデータとして6チャンネルのオーディオデータを伝送する場合のパケット構造例を示しているものである。

なお、図7にフレームとして示すブロック#0～#1567の部分は、図3、図4で説明したアイソクロナスパケットIso内のデータ部に相当する部分である。

#### 【0046】

6チャンネルデータの場合、8カドレット(q1～q8)で1つのブロックが形成され、このブロックが連続するものとなる。

1 5 6 8 ブロックの範囲が 1 フレームとなる。

そして 1 ビットデジタルオーディオデータとしての伝送データストリームは、このようなフレームが連続されて形成される。

【 0 0 4 7 】

この場合、ブロック # 0 の第 1 カドレット q 1 をみると、ラベル値は「D 1 h」とされている。従って第 1 カドレット q 1 はアンシラリデータが記述されるものと提示されていることになり、さらにこの場合バイト 1 はサブラベルとされて「0 0 h」とされている。図 3 で説明したように、バイト 2、バイト 3 の補助データ内容としては、コピーコントロール情報、チャンネル数、スピーカ配置情報等が記述される。

【 0 0 4 8 】

第 2 カドレット q 2 ではラベル値は「5 0 h」とされる。ラベル値 5 0 h ~ 5 7 h は、1 ビットデジタルオーディオデータに対応する値であるが、「5 0 h」は、マルチチャンネルのデータを配したブロックの最初のデータであることを示す。

また第 3 ~ 第 7 カドレット (q 3 ~ q 7) ではラベル値は「5 1 h」とされる。「5 1 h」は、マルチチャンネルのデータを配したブロックの 2 番目以降のデータであることを示す。

従って、第 2 ~ 第 7 カドレット (q 1 ~ q 7) では、チャンネル 1 ~ チャンネル 6 の 6 チャンネルの 1 ビットデジタルオーディオデータが配されていることが示されるものとなる。各チャンネルのデータはバイト 1 ~ バイト 3 の 3 バイトで記述される。

【 0 0 4 9 】

第 8 カドレット q 8 では、ラベル値は「C F h」とされている。これはアンシラリデータの範疇であるが、「C F h」は特に無効データ (NO DATA) を示す値として定義されている。

またこの場合は、バイト 1 は無効データの内容を示す値とされており、この例のような「5 0 h」は 1 ビットデジタルオーディオデータとしての無効データを示すものとなる。

そしてこのときバイト2, バイト3が無効データにより充填される。

【0050】

ブロック#1の第1カドレットq1では、ラベル値は「D1h」とされている。従って第1カドレットq1はアンシラリデータが記述されるものと提示されていることになり、さらにこの場合バイト1はサブラベルとされて「01h」とされている。

このときはバイト2, バイト3の補助データ内容は、サプリメンタリデータとされる。

第2～第8カドレットはブロック#0と同様である。

【0051】

ブロック#1567の第1カドレットq1では、ラベル値は「CFh」とされている。つまりバイト2, バイト3は無効データである。ただし、バイト1は「D1h」とされていることで、アンシラリデータとしての無効データであることが示されている。

第2～第8カドレットはブロック#0と同様である。

【0052】

例えばこのようなパケットデータストリームを伝送する場合を例に挙げると、上述した送信装置1のランダムノイズ付加部11では、図7のような連続するブロックによって構成されるトラックの先頭及び終端に、図8のようなブロックを任意の長さ（ランダムなデータ量）だけ付加するものとなる。

【0053】

図8のブロックは、図7と同じく8カドレット(q1～q8)で構成されるが、全てのカドレットは、ラベルが「CFh」とされている。即ち無効データであることが示される。またサブラベルとして、「D1h」「50h」「CFh」等が配される。

そして全カドレットq1～q8のバイト2, 3（斜線部）には、ランダムノイズが充填される。

【0054】

このようなランダムノイズが充填されたブロックをトラックの先頭及び終端に

任意のブロック数だけ付加することで、図 2 (c) に示したような状態とする。  
そして上述した図 2 (d) のように暗号化が施されて送出される。

これによって、伝送される暗号化データ D T s から仮にトラックの先頭又は終端に相当する部分が抽出されたとしても、その部分は暗号化前のデータがランダムノイズであるため、上述の通り、暗号解読を防止できるものとなる。

#### 【 0 0 5 5 】

また、このように無効データであることを示すラベル「C F h」を設定したブロック内の各カドレットにランダムノイズを配することは、受信装置 2 側での処理が非常に簡単となることを意味する。

即ち受信装置 1 0 2 の復号部 2 2 で暗号解読処理が施されると、図 7，図 8 の状態の packets データストリームがランダムノイズ除去部 2 3 に供給されることになるが、ランダムノイズ除去部 2 3 では、ラベル値＝「C F h」のカドレットを捨てればよいのみとなる。

ラベル値＝「C F h」のカドレットは無効データとして本来捨てられるものであるため、その意味でいえば、ランダムノイズ除去部 2 3 は何ら特別な処理を必要とせずに、図 7 における無効データとともに、図 8 におけるランダムノイズを除去できるものともなる。

#### 【 0 0 5 6 】

### 4. 記録装置及び再生装置に本発明を採用する例

続いて、本発明のデータ送出装置（データ送出方法）、データ復号装置（データ復号方法）を、記録装置、再生装置に採用する実施の形態を説明する。

記録装置は記録媒体に対するデータ送出装置となり、また再生装置は記録媒体から読み出されたデータのデータ復号装置となる。

#### 【 0 0 5 7 】

図 9 は所定の記録媒体（メディア） 6 に対してデータ D T を記録できる記録装置である。

図示するように記録装置 4 は、入力されてくるデータ D T に対する記録処理系として、暗号化部 4 0、エンコード及び記録ドライブ部 4 4、記録ヘッド（又はインターフェース） 4 5 が設けられる。

暗号化部 4 0 は、ランダムノイズ付加部 4 1、暗号化部 4 2、送出部 4 3、ランダムノイズ発生部 4 6 を有する。

#### 【 0 0 5 8 】

このような記録装置 4 では、入力されたデータ D T について、ランダムノイズ付加部 4 1 は、ランダムノイズ発生部 4 6 から発生させたランダムノイズを、データ D T におけるトラック（プログラム）の先頭及び終端部分に付加する。この場合も付加するランダムノイズのデータ長は可変長とすることで、暗号解読の困難性を高めることができる。

ランダムノイズ付加部 4 1 でランダムノイズが付加されたデータ D T a d は、続いて暗号化部 4 2 に供給され、暗号化処理が施される。

暗号化されたデータ D T s は、送出部 4 3 に供給され、送出部 4 3 からエンコード及び記録ドライブ部 4 4 に送出される。

#### 【 0 0 5 9 】

エンコード及び記録ドライブ部 4 4 は、供給されたデータ D T s に対して、記録を行うメディア 6 の記録フォーマット、変調方式に応じてエラー訂正符号の付加や各種エンコード処理を行い、記録ドライブ信号を生成する。

その記録ドライブ信号は記録ヘッド 4 5 に供給されて記録ヘッド 4 5 によりメディア 6 へのデータ書込が行われる。

例えばメディア 6 が光ディスク、光磁気ディスク、磁気ディスク、磁気テープなどであれば、記録ドライブ信号に応じて光学ヘッド又は磁気ヘッドが駆動されて記録が実行される。

また、メディア 6 がフラッシュメモリなどによるメモリカードのような形態であれば、インターフェース 4 5 によりメディア 6 に対して書込アクセスが行われることになる。

#### 【 0 0 6 0 】

図 1 0 は所定の記録媒体（メディア） 6 からデータ D T を再生できる再生装置



である。

図示するように再生装置 5 は、メディア 6 からデータの読み出しを行う再生ヘッド（又はインターフェース）5 4、デコード部 5 5、復号部 5 0 が設けられる。

復号部 5 0 は、取込部 5 1、復号部 5 2、ランダムノイズ除去部 5 3 を備える。

#### 【0061】

この再生装置 5 では、例えばメディア 6 としての光ディスク、光磁気ディスク、磁気ディスク、磁気テープなどから光学ヘッド又は磁気ヘッドとしての再生ヘッド 5 4 によって読み出されたデータ、或いはメディア 6 としてのメモリカードからインターフェース 5 4 を介した読出アクセスにより読み出されたデータは、デコード部 5 5 で、メディア 6 の記録フォーマットに応じたデコード処理やエラー訂正処理が行われる。そしてそのデコードされたデータは、即ち記録装置 4 で暗号化されたデータ D T s であり、データ D T s は取込部 5 1 により復号部 5 0 内に取り込まれ、復号部 5 2 で暗号解読処理される。

復号部 5 2 で、上記暗号化部 4 2 での暗号化アルゴリズムに対応した暗号解読処理を行うことで、ランダムノイズが付加された状態のデータ D T a d とされる。そして、そのデータ D T a d がランダムノイズ除去部 5 3 に供給されて、上記ランダムノイズ付加部 4 1 で付加されたランダムノイズ部分が除去されることで、元のデータ D T が再生されるものとなる。

#### 【0062】

記録装置 4、再生装置 5 が以上のように構成されることで、メディア 6 に記録されるデータは、トラックの先頭及び終端にランダムノイズが付加された上で暗号化されたデータ D T s がエンコードされたものである。つまりトラックの先頭及び終端はゼロデータ又は「9 6 h」等の固定データが連続する状態ではないようにされた上で暗号化されたデータが、エンコードされている。

従ってメディア 6 に記録されたデータをデコードしても、トラックの先頭又は終端は無音部分ではなくなる。このため、その部分が抽出され、データ D T s が解析されたとしても、データ D T s 上では暗号化アルゴリズムによるデータ要素

とランダムノイズによるデータ要素を区別することはできず、暗号化アルゴリズムを解析することはほぼ不可能である。

#### 【 0 0 6 3 】

つまりこのような記録装置、再生装置によれば、メディア 6 に記録されるデータについて暗号解読は非常に困難なものとなり、従って、著作権保護を要するデータの記録などに非常に好適なものとなる。また、上述した送信装置 1，受信装置 2 の場合と同様に、記録装置 4、再生装置 5 として構成がさほど複雑化することもなく、導入は容易である。

#### 【 0 0 6 4 】

なお、図 9，図 1 0 として記録装置 4、再生装置 5 を分けて示したが、これらの回路構成を 1 つの機器に設けて、記録再生装置とすることはもちろん可能である。

また、記録装置 4（又は記録再生装置）としては、必ずしも暗号化部 4 0 を設けなくてもよい。例えば伝送路 3 を介して或る送信装置から伝送されてきたデータを記録する記録装置を考えると、その送信装置側が図 1 に示した構成を備えていれば、記録装置に伝送されてくるデータは、既にランダムノイズが付加された上で暗号化されたデータ D T s となっている。従ってその場合、記録装置は暗号化部 4 0 は不要となる。そして再生装置は、図 1 0 に示した復号部 5 0 を備えることで、伝送され記録されたデータの再生を行うことができるようになる。

例えば音楽等の配信システムなどを想定すると、このような形態が好適なものとなる。

#### 【 0 0 6 5 】

以上、実施の形態を説明してきたが、本発明はさらに多様な構成例が考えられ、また送信装置、受信装置、記録装置、再生装置などの形態で多種多様な機器に導入できるものである。

また、上記例では送信装置 1 と受信装置 2 は有線としての I E E E 1 3 9 4 方式の伝送路 3 による伝送システムとしたが、他の伝送規格によるものでもよく、また衛星通信、無線電話通信、赤外線伝送などの無線伝送システムに本発明を適用できることはもちろんである。

また、伝送するデータは図 7、図 8 に示したようなブロックデータに限定されるものではなく、あらゆるデータの伝送に本発明を適用できる。

#### 【 0 0 6 6 】

##### 【発明の効果】

以上の説明からわかるように、本発明によれば、伝送するプログラムデータについて、その前後にランダムノイズを付加したうえで暗号化を行なって伝送するようにしている。このため、例えば元の曲データ等においてその先頭又は終端が無音データとしてゼロデータ列などの内容が明確な部分が存在しても、その状態が解消された上で、つまり先頭及び終端がランダムデータとされた上で、暗号化されることとなるため、伝送過程などで暗号化データが抽出されたとしても、暗号アルゴリズムの解読は非常に困難なものとなるという効果があり、従って著作権保護などに好適なものとなる。

また、このようにランダムノイズが付加された上で暗号化されたデータを復号する場合は、暗号化を解読したうえでランダムノイズが挿入されたデータ部分を除去するのみでデータを復号できるため、復号のために複雑な処理は必要なく、簡易な構成で復号装置を実現できる。

換言すれば本発明では、データ送出装置、データ復号装置としては装置構成の複雑化を招かずに、暗号解読が非常に困難なデータ伝送を実現できるものとなる。

#### 【 0 0 6 7 】

また本発明では、データ送出装置側で付加するランダムノイズのデータ長は可変長とすることで、実際の無音データ部分が予測困難となる。これによって暗号解読防止機能を一層高めることができる。

#### 【 0 0 6 8 】

またデータ送出装置とデータ復号装置は、それぞれ異なる機器間における送信装置、受信装置とすることで、機器間のデータ伝送において上記効果を実現できる。

さらにデータ送出装置とデータ復号装置は、それぞれ記録媒体に記録を行う記録装置における記録データの送出装置、記録媒体からデータの再生を行う再生装

置における再生データの復号装置とすることで、記録媒体に記録されているデータ、又は記録再生の過程のデータにおいて上記効果を実現できる。

【図面の簡単な説明】

【図 1】

本発明の実施の形態の送信装置及び受信装置のブロック図である。

【図 2】

実施の形態のランダムノイズ付加の説明図である。

【図 3】

I E E E 1 3 9 4 による伝送フォーマットの説明図である。

【図 4】

I E E E 1 3 9 4 のアイソクロナスパケットの説明図である。

【図 5】

実施の形態のパケットデータのラベルの説明図である。

【図 6】

実施の形態のトラック構造の説明図である。

【図 7】

実施の形態のランダムノイズ付加例の説明図である。

【図 8】

実施の形態のランダムノイズ付加例の説明図である。

【図 9】

実施の形態の記録装置のブロック図である。

【図 1 0】

実施の形態の再生装置のブロック図である。

【図 1 1】

従来の伝送システムの説明図である。

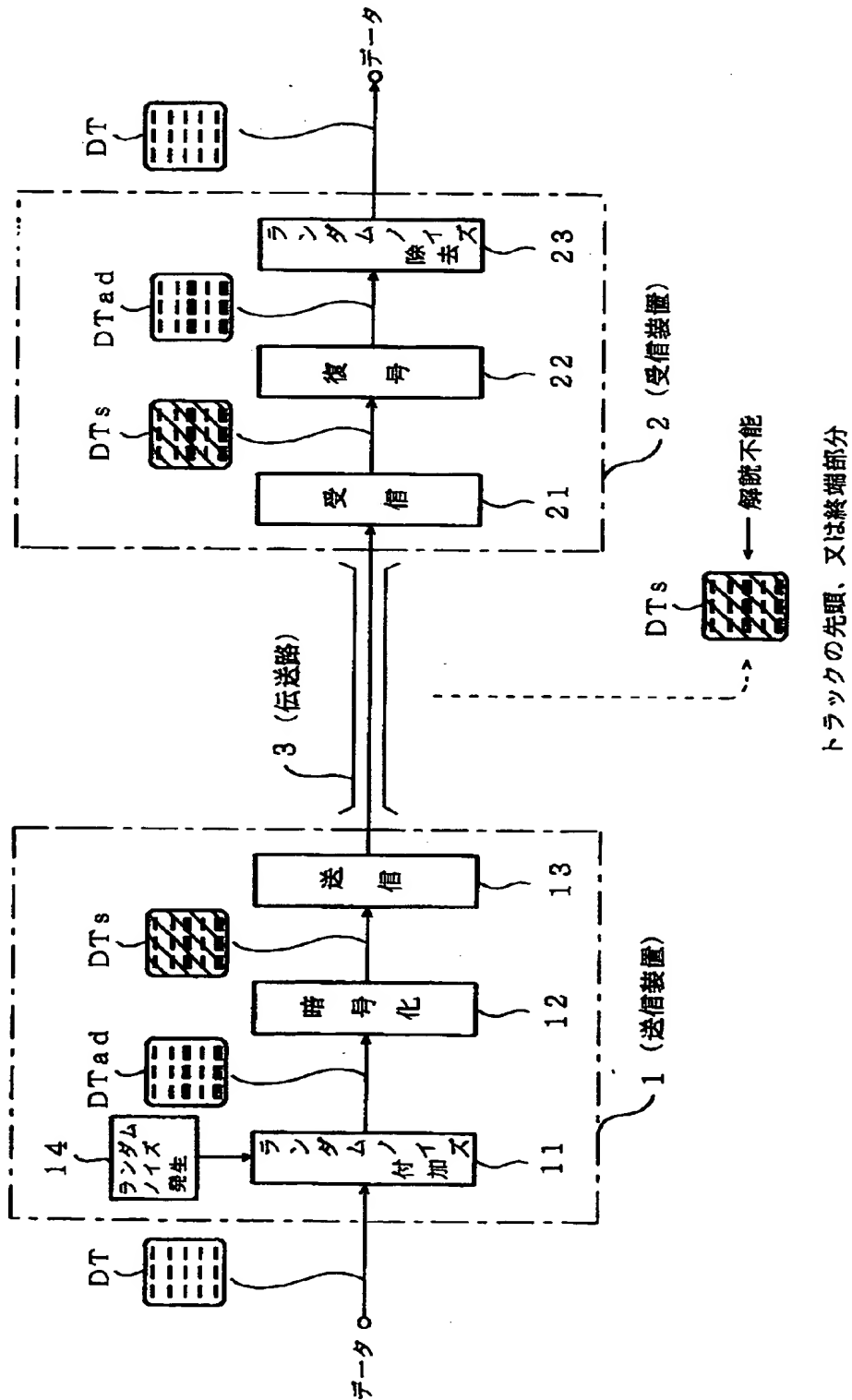
【符号の説明】

1 送信装置、2 受信装置、3 伝送路、4 記録装置、5 再生装置、6  
メディア、11, 41 ランダムノイズ付加部、12, 42 暗号化部、13  
送信部、14, 46 ランダムノイズ発生部、21 受信部、22, 52 復

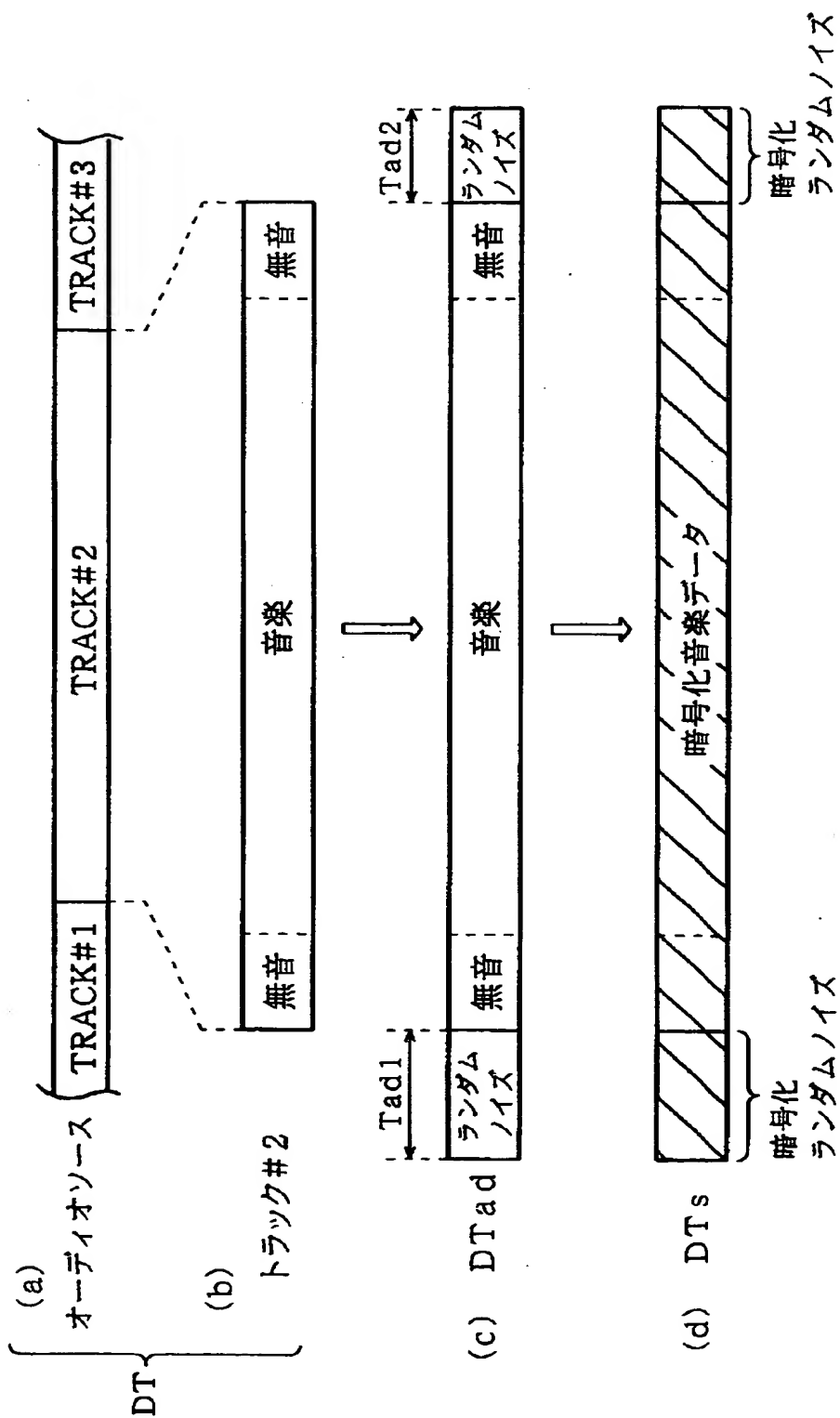
号部、2 3, 5 3 ランダムノイズ除去部、4 3 送出部、5 1 取込部

【書類名】 図面

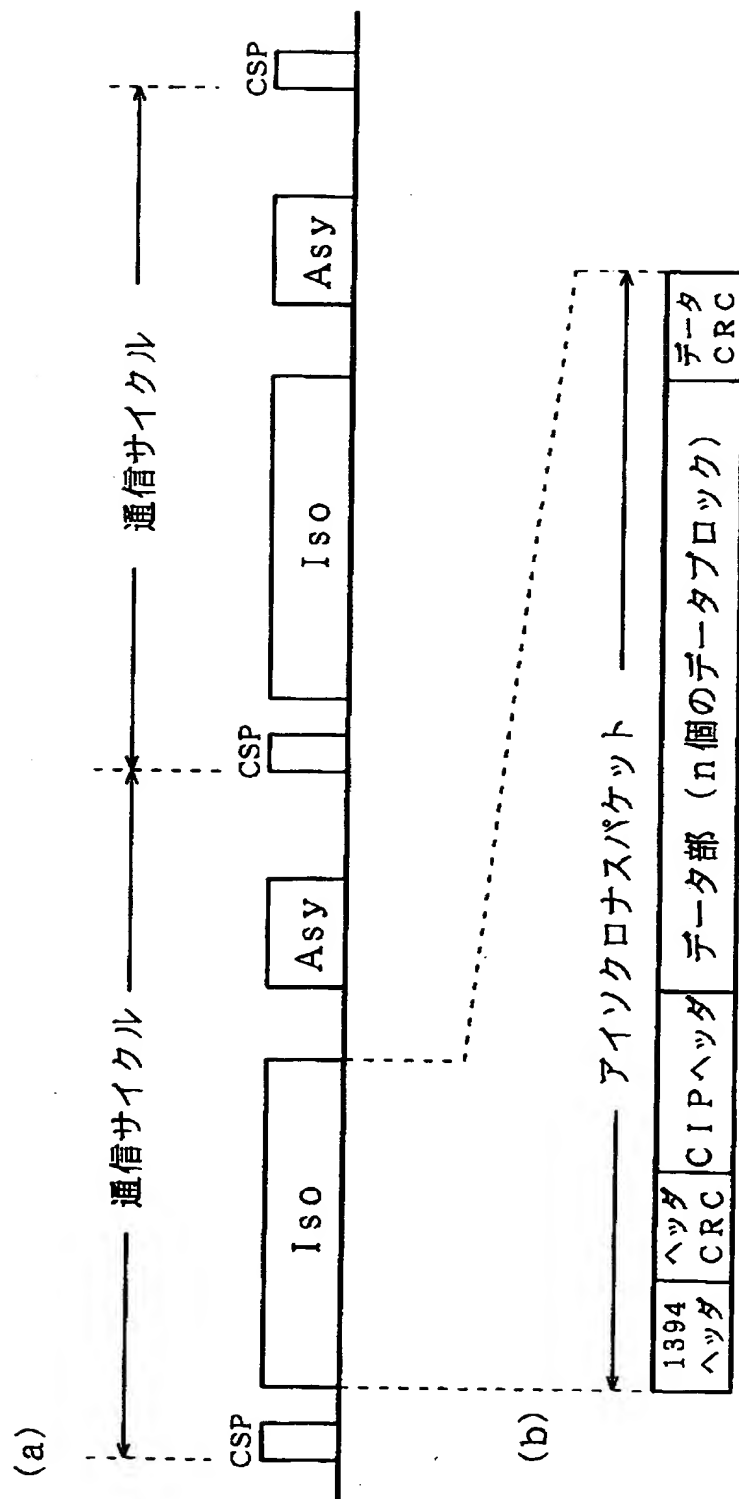
【図 1】



【図2】

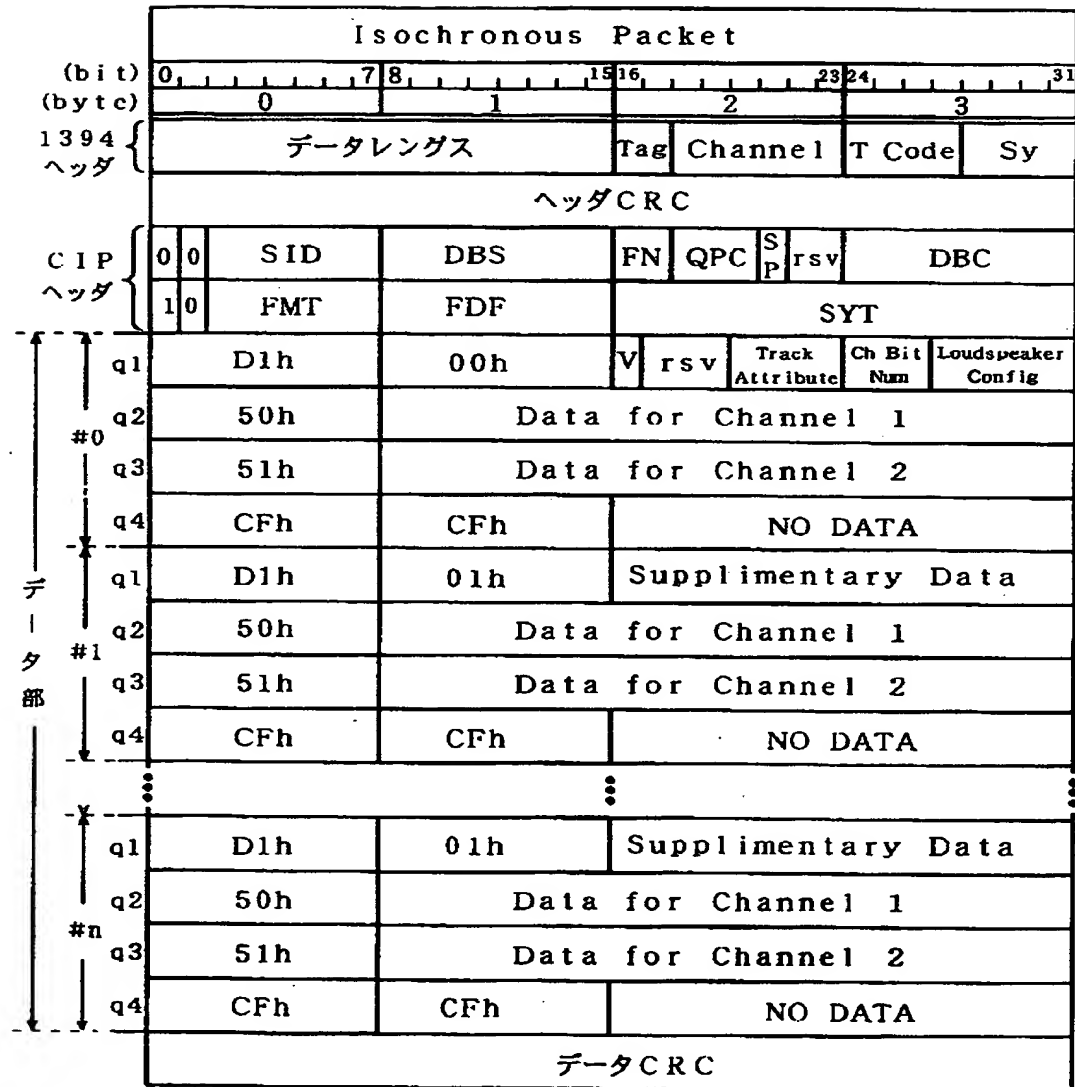


【図3】





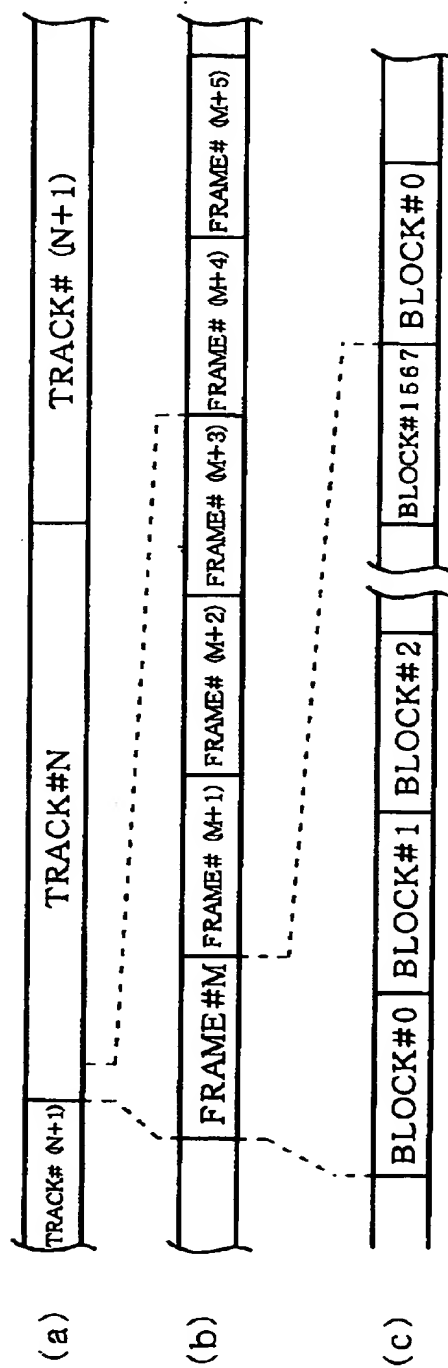
【図4】



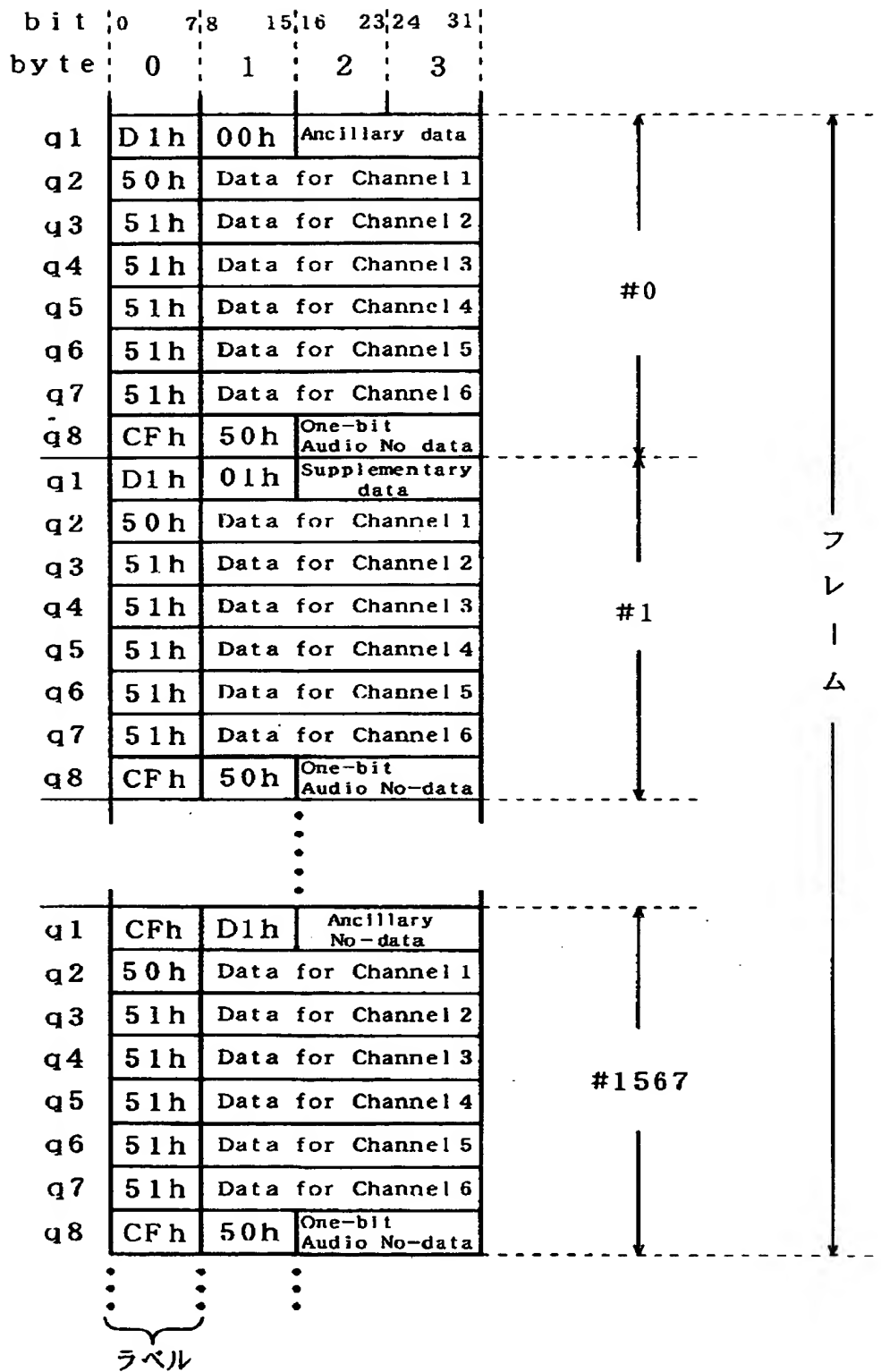
【図5】

Value	Description
00h-3Fh	IEC60958 Conformant
40h-4Fh	Multi-bit Linear Audio
50h-57h	One Bit Audio (Plain)
58h-5Fh	One Bit Audio (Encoded)
60h-7Fh	-reserved-
80h-83h	MIDI Conformant
84h-87h	Extended Music Data
88h-8Bh	SMPTE Time Code Conformant
8Ch-8Fh	Sample Count
90h-BFh	-reserved-
C0h-EFh	Ancillary Data
F0h-FFh	-reserved-

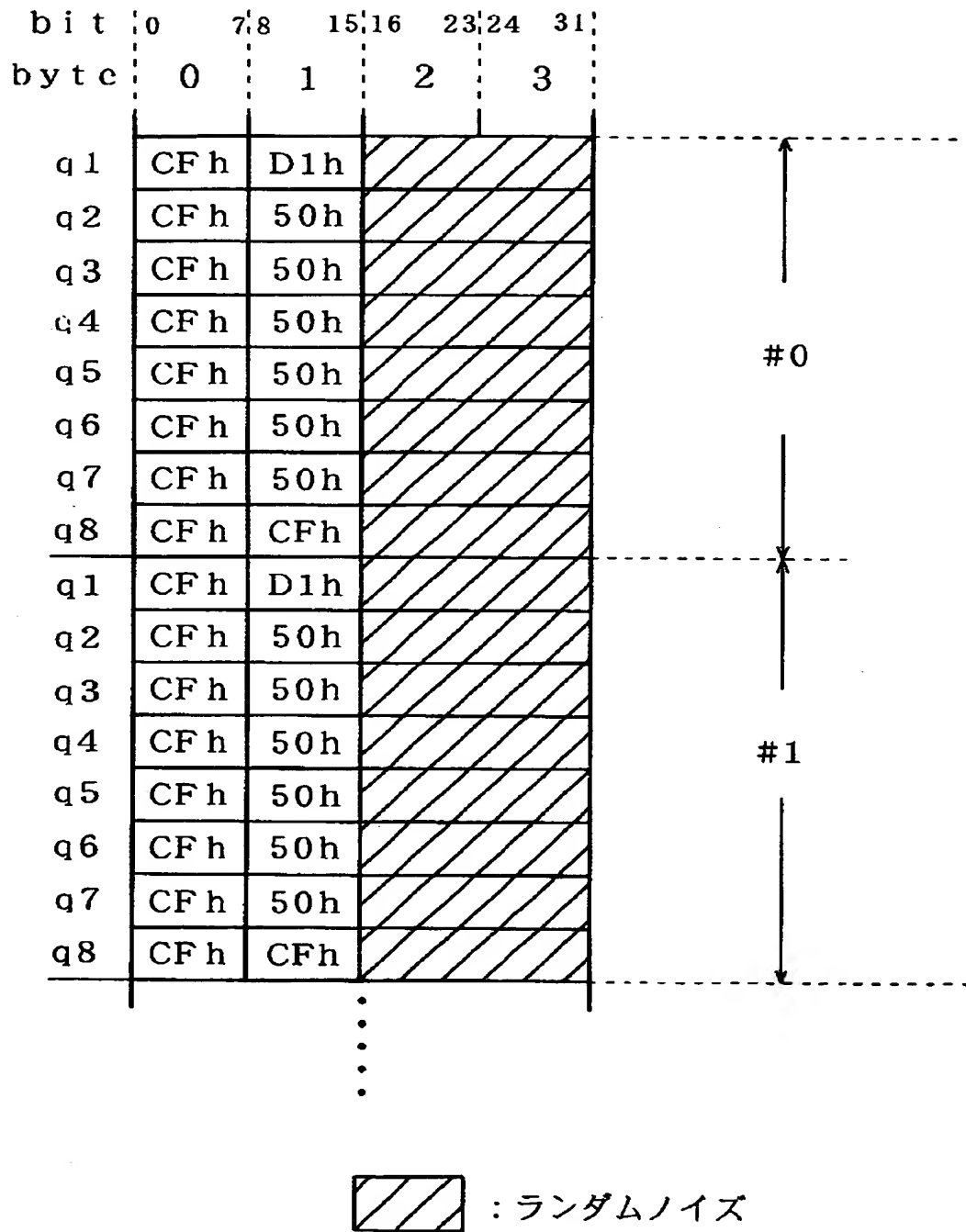
【図 6】



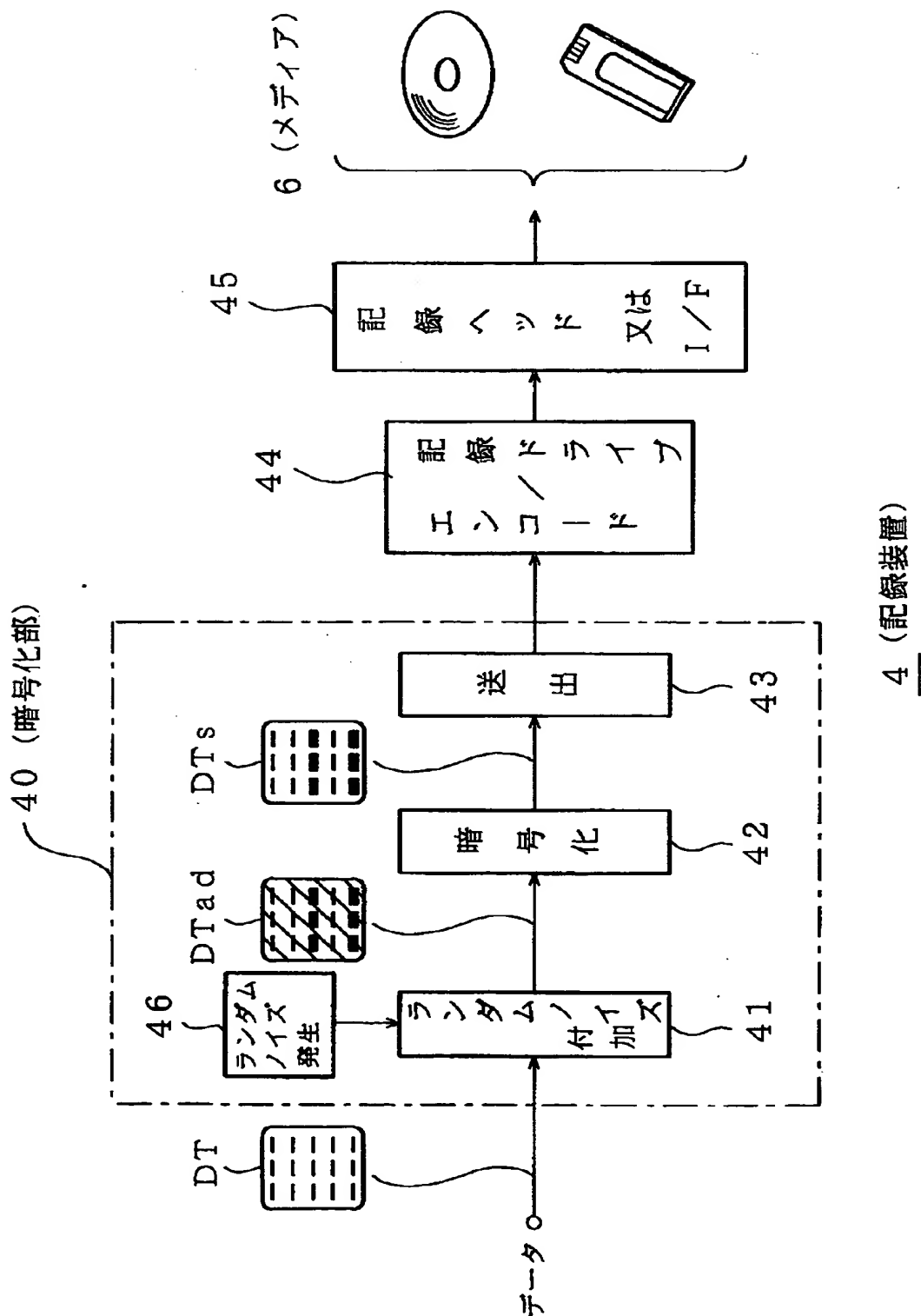
【図 7】



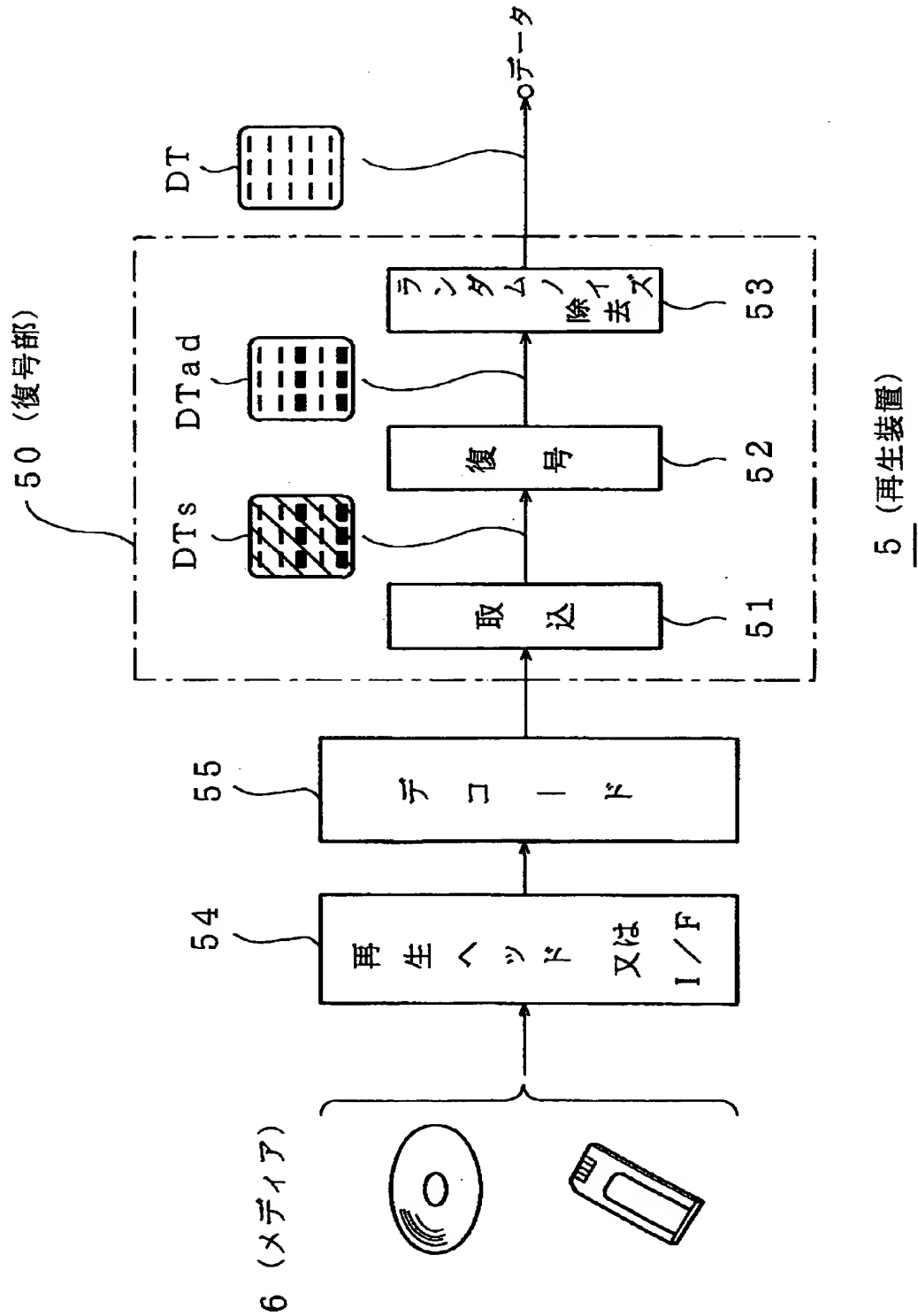
【図 8】



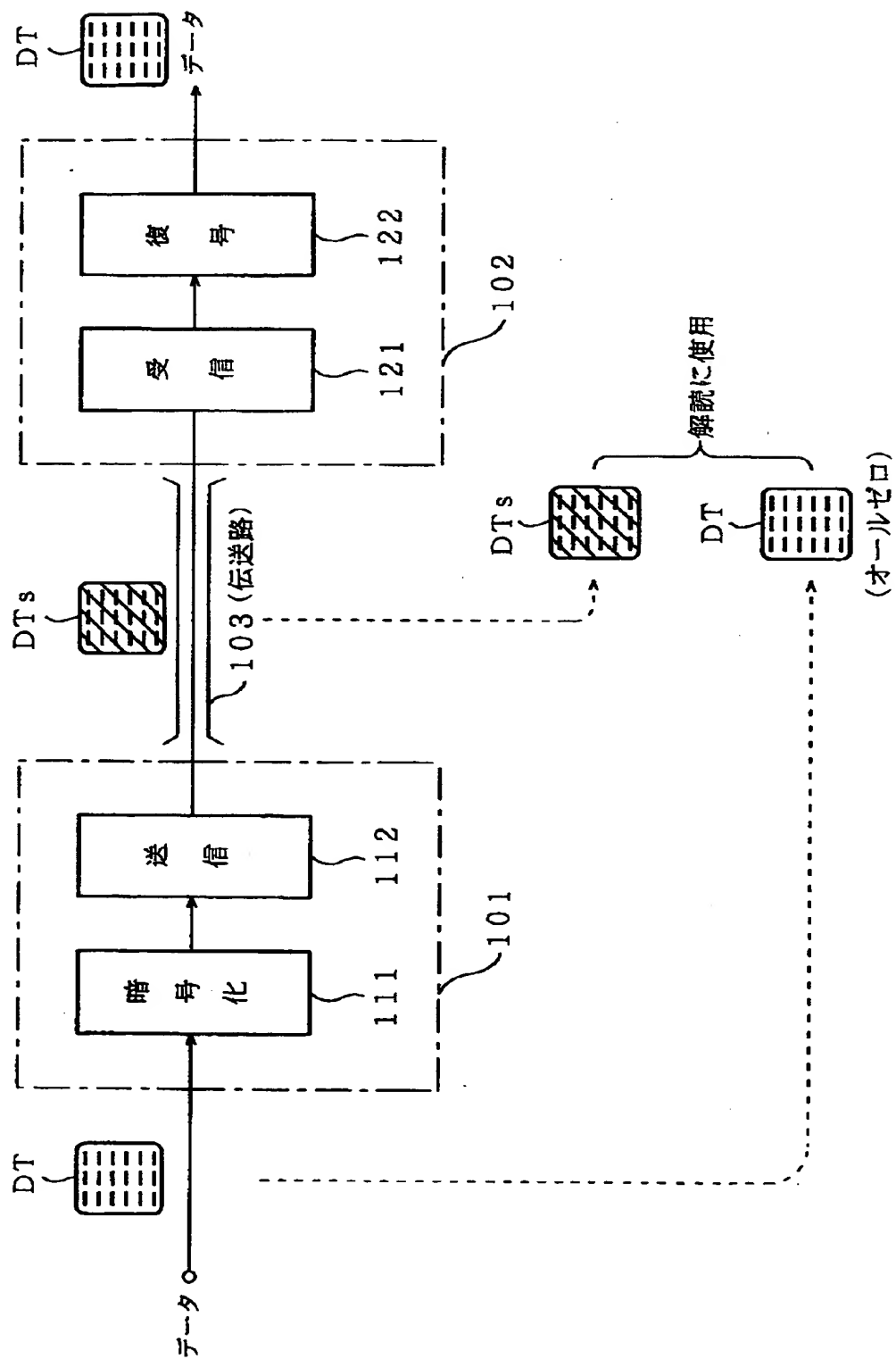
【図9】



【図10】



【図 11】





【書類名】            要約書

【要約】

【課題】    暗号解読が困難で著作権保護などに好適なデータ伝送の実現。

【解決手段】    伝送するプログラムデータについて、その前後にランダムノイズを付加したうえで暗号化を行なって伝送し、伝送過程などで暗号化データが抽出されたとしても、暗号アルゴリズムの解読を困難なものとする。データの復号は、暗号化を解読したうえでランダムノイズが付加されたデータ部分を除去することで行う。

【選択図】            図 2

認定・付加情報

特許出願の番号	特願 2000-260864
受付番号	50005044299
書類名	特許願
担当官	風戸 勝利 9083
作成日	平成 12 年 8 月 30 日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000002185
【住所又は居所】	東京都品川区北品川 6 丁目 7 番 35 号
【氏名又は名称】	ソニー株式会社

【代理人】

申請人

【識別番号】	100086841
【住所又は居所】	東京都中央区新川 1 丁目 27 番 8 号 新川大原ビル 6 階

【氏名又は名称】	脇 篤夫
----------	------

【代理人】

【識別番号】	100114122
【住所又は居所】	東京都中央区新川 1 丁目 27 番 8 号 新川大原ビル 6 階 脇特許事務所

【氏名又は名称】	鈴木 伸夫
----------	-------

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都品川区北品川6丁目7番35号
氏 名	ソニー株式会社